(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2002－319934
（P2002－319934A）
(43)公開日　平成14年10月31日(2002.10.31)

(51)Int.Cl.⁷	識別記号	ＦＩ		テーマコード(参考)
Ｈ０４Ｌ　9/32		Ｇ０６Ｆ　12/14	３２０Ｂ	５Ｂ０１７
Ｇ０６Ｆ　12/14	３２０	Ｈ０４Ｌ　9/00	６７５Ａ	５Ｊ１０４
Ｈ０４Ｌ　9/08			６０１Ｂ	

審査請求　有　　請求項の数15　ＯＬ　（全 11 頁）

(21)出願番号　特願2001－121061(P2001－121061)

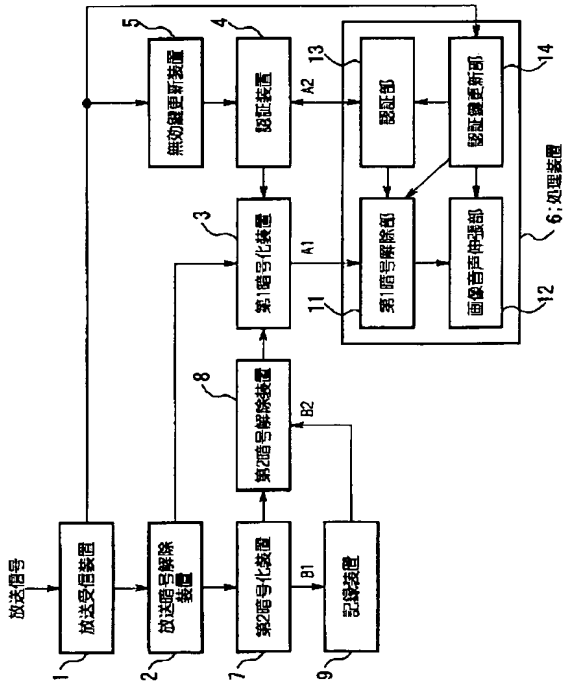
(22)出願日　平成13年４月19日(2001.4.19)

(71)出願人　000004237
日本電気株式会社
東京都港区芝五丁目７番１号
(72)発明者　森下　卓也
東京都港区芝五丁目７番１号　日本電気株式会社内
(72)発明者　宮内　宏
東京都港区芝五丁目７番１号　日本電気株式会社内
(74)代理人　100108578
弁理士　高橋　詔男　（外３名）

最終頁に続く

(54)【発明の名称】　著作権保護システム及びその方法

(57)【要約】
【課題】　自システム内の暗号に係る鍵を無効化することが可能な著作権保護システムを実現する。
【解決手段】　暗号に係る鍵の無効情報を有し、第１暗号化装置３と第１暗号解除部１１の間で暗号化に係る第１の暗号鍵を共有する際の認証に使用する認証鍵の情報がその無効情報の中に含まれる場合に、当該認証を不可とする認証装置４と、著作物に係る入力データに付随して提供される無効化対象の鍵の情報を受け取ると、認証装置４の無効情報の内容を更新する無効鍵更新装置５とを具備することを特徴とする。



1

【特許請求の範囲】

【請求項１】 著作物に係る入力データを暗号化することによって該著作物の著作権を保護する著作権保護システムであって、

暗号に係る鍵の無効情報を有し、第１の暗号化手段と第１の暗号解除手段の間で前記暗号化に係る第１の暗号鍵を共有する際の認証に使用する認証鍵の情報が前記無効情報の中に含まれる場合に、前記認証を不可とする認証手段と、

前記入力データに付随して提供される無効化対象の鍵の情報を受け取ると、前記無効情報の内容を更新する無効情報更新手段と、を具備することを特徴とする著作権保護システム。

【請求項２】 前記入力データに付随して提供される更新用認証鍵を受け取ると、前記認証鍵を更新する認証鍵更新手段を備えることを特徴とする請求項１に記載の著作権保護システム。

【請求項３】 前記暗号化の解除に係る機能を実現するための処理プログラムを実行する処理装置を備え、

前記処理装置は、前記入力データに付随して提供される更新用プログラムを受け取ると、前記処理プログラムを更新することを特徴とする請求項１または請求項２に記載の著作権保護システム。

【請求項４】 第２の暗号鍵を使用して前記入力データを暗号化し、該第２の暗号データを記録媒体に記録する第２の暗号化手段を備えることを特徴とする請求項１乃至請求項３のいずれかの項に記載の著作権保護システム。

【請求項５】 前記第２の暗号データの暗号を前記第２の暗号鍵により解除する第２の暗号解除手段を備え、

前記第２の暗号鍵を自システム内に保持することを特徴とする請求項４に記載の著作権保護システム。

【請求項６】 著作物に係る入力データを暗号化することによって該著作物の著作権を保護する著作権保護システムにおける著作権保護方法であって、

第１の暗号化手段と第１の暗号解除手段の間で前記暗号化に係る第１の暗号鍵を共有する際に認証を行う過程と、

この認証に使用する認証鍵の情報が暗号に係る鍵の無効情報の中に含まれる場合に、前記認証を不可とする過程と、

前記入力データに付随して提供される無効化対象の鍵の情報を受け取ると、前記無効情報の内容を更新する過程と、を含むことを特徴とする著作権保護方法。

【請求項７】 前記入力データに付随して提供される更新用認証鍵を受け取ると、前記認証鍵を更新する過程をさらに含むことを特徴とする請求項６に記載の著作権保護方法。

【請求項８】 前記入力データに付随して提供される更新用プログラムを受け取る過程と、

2

この更新用プログラムにより、前記暗号化の解除に係る機能を実現するための処理プログラムを更新する過程と、をさらに含むことを特徴とする請求項６または請求項７に記載の著作権保護方法。

【請求項９】 第２の暗号鍵を使用して前記入力データを暗号化する過程と、

該第２の暗号データを記録媒体に記録する過程と、をさらに含むことを特徴とする請求項６乃至請求項８のいずれかの項に記載の著作権保護方法。

【請求項１０】 前記第２の暗号鍵を自システム内に保持する過程と、

前記第２の暗号データの暗号を自システム内に保持された第２の暗号鍵により解除する過程と、をさらに含むことを特徴とする請求項９に記載の著作権保護方法。

【請求項１１】 著作物に係る入力データを暗号化することによって該著作物の著作権を保護する著作権保護システムにおける著作権保護処理を行うための著作権保護プログラムであって、

第１の暗号化手段と第１の暗号解除手段の間で前記暗号化に係る第１の暗号鍵を共有する際に認証を行う処理と、

この認証に使用する認証鍵の情報が暗号に係る鍵の無効情報の中に含まれる場合に、前記認証を不可とする処理と、

前記入力データに付随して提供される無効化対象の鍵の情報を受け取ると、前記無効情報の内容を更新する処理と、をコンピュータに実行させることを特徴とする著作権保護プログラム。

【請求項１２】 第２の暗号鍵を使用して前記入力データを暗号化する処理と、

該第２の暗号データを記録媒体に記録する処理と、をさらにコンピュータに実行させることを特徴とする請求項１１に記載の著作権保護プログラム。

【請求項１３】 前記第２の暗号鍵を自システム内に保持する処理と、

前記第２の暗号データの暗号を自システム内に保持された第２の暗号鍵により解除する処理と、

をさらにコンピュータに実行させることを特徴とする請求項１２に記載の著作権保護プログラム。

【請求項１４】 著作物に係る入力データを暗号化することによって該著作物の著作権を保護する著作権保護システムにおける著作権保護処理を行うための著作権保護プログラムであって、

前記入力データに付随して提供される更新用認証鍵を受け取り、認証鍵を更新する処理をコンピュータに実行させることを特徴とする著作権保護プログラム。

【請求項１５】 前記入力データに付随して提供される更新用プログラムを受け取る処理と、

この更新用プログラムにより、前記暗号化の解除に係る機能を実現するための処理プログラムを更新する処理

と、をさらにコンピュータに実行させることを特徴とする請求項１４に記載の著作権保護プログラム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、放送等により提供される著作物の著作権を暗号化により保護する著作権保護システム及びその方法に関する。

【０００２】

【従来の技術】図３は、従来の著作権保護システムの構成例を示すブロック図である。この図３に示す著作権保護システムは、ＤＶＤ（Digital Versatile Disc）に記録された著作物の著作権を保護するためのものである。一般に、著作物をＤＶＤに記録して販売する際には、悪意を持った第三者により著作物が不正に使用されることを防止するために、画像や音声など著作物のデータは暗号化された後、ＤＶＤに記録される。また、その記録データの暗号解除に必要なディスク鍵とタイトル鍵も暗号化されてＤＶＤに記録される。

【０００３】図３の従来の著作権保護システムは、ＤＶＤ読出し装置２１、バス２２、バス認証部２３、マスター鍵２４、ディスク鍵復号部２５、タイトル鍵復号部２６、デスクランブル部２７、及びＭＰＥＧデコーダ２８を備える。ＤＶＤ読出し装置２１とバス認証部２３とデスクランブル部２７はそれぞれバス２２に接続されており、このバス２２を介してデータ伝送が可能である。バス認証部２３とデスクランブル部２７は、ＤＶＤ読出し装置２１によってＤＶＤから読み出されたデータをバス２２を介して取得する。

【０００４】次に、上記図３に示す従来の著作権保護システムの動作を説明する。先ず、バス認証部２３はバス２２を介してＤＶＤ読出し装置２１との間で相互認証を行い、バス２２を介して鍵を伝送するための時変鍵を共有する。次いで、バス認証部２３は、ＤＶＤ読出し装置２１によりＤＶＤから暗号化されたディスク鍵とタイトル鍵を読み出して取得し、そのディスク鍵をディスク鍵復号部２５へ提供し、またタイトル鍵をタイトル鍵復号部２６へ提供する。ディスク鍵復号部２５はマスター鍵２４によりディスク鍵の暗号を解除してディスク鍵を復号する。タイトル鍵復号部２６はディスク鍵復号部２５から復号されたディスク鍵を取得し、このディスク鍵によりタイトル鍵の暗号を解除してタイトル鍵を復号し、このタイトル鍵をデスクランブル部２７へ提供する。

【０００５】次いで、デスクランブル部２７は、ＤＶＤ読出し装置２１によりＤＶＤから暗号化された著作物のデータの暗号をタイトル鍵により解除してＭＰＥＧデコーダ２８へ出力する。ＭＰＥＧデコーダ２８は、その暗号が解除されたデータを使用して画像または音声を再生する。

【０００６】上述したように従来の著作権保護システムにおいては、ＤＶＤに記録されているディスク鍵とタイトル鍵の暗号解除に必要なマスター鍵を備え、このマスター鍵なしではディスク鍵とタイトル鍵を復号してＤＶＤに記録されている著作物のデータの暗号を解除することができないようにしている。また、バス２２上で伝送されるデータは暗号化されたものなので、バス２２からデータを取得してもそのデータから再生可能な著作物のデータを取得することは困難である。このようにして従来の著作権保護システムは、悪意を持った第三者により著作物が不正に使用されることを防止するものである。

【０００７】また、上記図３の著作権保護システムは、プログラムを実行可能な処理装置を備えるようにし、この処理装置が各部２３及び２５～２８のそれぞれの機能を実現するためのプログラムを実行して各部２３及び２５～２８を実現することも可能である。これにより、パーソナルコンピュータ等の情報処理装置に図３の著作権保護システムを備えることが可能となっている。

【０００８】

【発明が解決しようとする課題】しかし、上述した従来の著作権保護システムでは、悪意を持った第三者によってプログラムの解析などにより認証方式や暗号化方式が解読された場合には、既に利用されている複数の著作権保護システムの暗号に係る鍵（マスター鍵）やプログラムを変更することは困難であり、著作物の不正使用を防止することができないという問題がある。

【０００９】このため、認証方式や暗号化方式などが解読されて著作物が不正に使用された場合に、著作権保護システムの暗号に係る鍵を無効化して、これ以上のさらなる著作物の不正使用を防止することが可能な著作権保護システムの実現が要望されている。

【００１０】また、放送番組の画像や音声など、放送により提供される著作物の著作権保護に関しては、その記録再生に対して対策がなされておらず、記録再生に係る著作権保護を実施可能な著作権保護システムの実現が要望されている。

【００１１】本発明は、このような事情を考慮してなされたもので、その目的は、自システム内の暗号に係る鍵を無効化することが可能な著作権保護システム及びその方法を提供することにある。また、その著作権保護システムをコンピュータを利用して実現するための著作権保護プログラムを提供することも目的とする。

【００１２】また、本発明は、複数の著作権保護システムにおいてそれらの暗号に係る鍵またはプログラムを簡易に変更することが可能な著作権保護システム及びその方法を提供することも目的とする。また、その著作権保護システムをコンピュータを利用して実現するための著作権保護プログラムを提供することも目的とする。

【００１３】また、本発明は、記録再生に係る著作権保護を実施可能な著作権保護システム及びその方法を提供することも目的とする。また、その著作権保護システムをコンピュータを利用して実現するための著作権保護プ

5

ログラムを提供することも目的とする。

【００１４】

【課題を解決するための手段】上記の課題を解決するために、請求項１に記載の発明は、著作物に係る入力データを暗号化することによって該著作物の著作権を保護する著作権保護システムであって、暗号に係る鍵の無効情報を有し、第１の暗号化手段と第１の暗号解除手段の間で前記暗号化に係る第１の暗号鍵を共有する際の認証に使用する認証鍵の情報が前記無効情報の中に含まれる場合に、前記認証を不可とする認証手段と、前記入力データに付随して提供される無効化対象の鍵の情報を受け取ると、前記無効情報の内容を更新する無効情報更新手段とを具備することを特徴とする。

【００１５】請求項２に記載の発明は、前記入力データに付随して提供される更新用認証鍵を受け取ると、前記認証鍵を更新する認証鍵更新手段を備えることを特徴とする請求項１に記載の著作権保護システムである。

【００１６】請求項３に記載の発明は、前記暗号化の解除に係る機能を実現するための処理プログラムを実行する処理装置を備え、前記処理装置は、前記入力データに付随して提供される更新用プログラムを受け取ると、前記処理プログラムを更新することを特徴とする請求項１または請求項２に記載の著作権保護システムである。

【００１７】請求項４に記載の発明は、第２の暗号鍵を使用して前記入力データを暗号化し、該第２の暗号データを記録媒体に記録する第２の暗号化手段を備えることを特徴とする請求項１乃至請求項３のいずれかの項に記載の著作権保護システムである。

【００１８】請求項５に記載の発明は、前記第２の暗号データの暗号を前記第２の暗号鍵により解除する第２の暗号解除手段を備え、前記第２の暗号鍵を自システム内に保持することを特徴とする請求項４に記載の著作権保護システムである。

【００１９】請求項６に記載の発明は、著作物に係る入力データを暗号化することによって該著作物の著作権を保護する著作権保護システムにおける著作権保護方法であって、第１の暗号化手段と第１の暗号解除手段の間で前記暗号化に係る第１の暗号鍵を共有する際に認証を行う過程と、この認証に使用する認証鍵の情報が暗号に係る鍵の無効情報の中に含まれる場合に、前記認証を不可とする過程と、前記入力データに付随して提供される無効化対象の鍵の情報を受け取ると、前記無効情報の内容を更新する過程とを含むことを特徴とする。

【００２０】請求項７に記載の発明は、前記入力データに付随して提供される更新用認証鍵を受け取ると、前記認証鍵を更新する過程をさらに含むことを特徴とする請求項６に記載の著作権保護方法である。

【００２１】請求項８に記載の発明は、前記入力データに付随して提供される更新用プログラムを受け取る過程と、この更新用プログラムにより、前記暗号化の解除に

6

係る機能を実現するための処理プログラムを更新する過程とをさらに含むことを特徴とする請求項６または請求項７に記載の著作権保護方法である。

【００２２】請求項９に記載の発明は、第２の暗号鍵を使用して前記入力データを暗号化する過程と、該第２の暗号データを記録媒体に記録する過程とをさらに含むことを特徴とする請求項６乃至請求項８のいずれかの項に記載の著作権保護方法である。

【００２３】請求項１０に記載の発明は、前記第２の暗号鍵を自システム内に保持する過程と、前記第２の暗号データの暗号を自システム内に保持された第２の暗号鍵により解除する過程とをさらに含むことを特徴とする請求項９に記載の著作権保護方法である。

【００２４】請求項１１に記載の発明は、著作物に係る入力データを暗号化することによって該著作物の著作権を保護する著作権保護システムにおける著作権保護処理を行うための著作権保護プログラムであって、第１の暗号化手段と第１の暗号解除手段の間で前記暗号化に係る第１の暗号鍵を共有する際に認証を行う処理と、この認証に使用する認証鍵の情報が暗号に係る鍵の無効情報の中に含まれる場合に、前記認証を不可とする処理と、前記入力データに付随して提供される無効化対象の鍵の情報を受け取ると、前記無効情報の内容を更新する処理とをコンピュータに実行させることを特徴とする。

【００２５】請求項１２に記載の発明は、第２の暗号鍵を使用して前記入力データを暗号化する処理と、該第２の暗号データを記録媒体に記録する処理とをさらにコンピュータに実行させることを特徴とする請求項１１に記載の著作権保護プログラムである。

【００２６】請求項１３に記載の発明は、前記第２の暗号鍵を自システム内に保持する処理と、前記第２の暗号データの暗号を自システム内に保持された第２の暗号鍵により解除する処理とをさらにコンピュータに実行させることを特徴とする請求項１２に記載の著作権保護プログラムである。

【００２７】請求項１４に記載の発明は、著作物に係る入力データを暗号化することによって該著作物の著作権を保護する著作権保護システムにおける著作権保護処理を行うための著作権保護プログラムであって、前記入力データに付随して提供される更新用認証鍵を受け取り、認証鍵を更新する処理をコンピュータに実行させることを特徴とする。

【００２８】請求項１５に記載の発明は、前記入力データに付随して提供される更新用プログラムを受け取る処理と、この更新用プログラムにより、前記暗号化の解除に係る機能を実現するための処理プログラムを更新する処理とをさらにコンピュータに実行させることを特徴とする請求項１４に記載の著作権保護プログラムである。

これらの著作権保護プログラムにより、前述の著作権保護システムがコンピュータを利用して実現できるように

なる。

【００２９】

【発明の実施の形態】以下、図面を参照し、本発明の一実施形態について説明する。図１は、本発明の一実施形態による著作権保護システムの構成を示すブロック図である。この図において、符号１は、放送信号を受信する放送受信装置である。この放送信号は、圧縮符号化され、さらに暗号化された画像データまたは音声データ（以下、圧縮暗号化データと称する）を含む。この暗号化は、視聴権利を有する者に対してのみ視聴可能とするためになされている。なお、上記放送信号は、テレビやラジオ等の無線放送やケーブルテレビ等の有線放送により伝送されるものであってもよく、あるいは、有線電話網や無線電話網、インターネット等の通信ネットワークを介して伝送されるものであってもよい。符号２は、放送受信装置１により受信された圧縮暗号化データの暗号を解除し、圧縮符号化された画像データまたは音声データ（以下、圧縮データと称する）を出力する放送暗号解除装置である。

【００３０】符号３は、放送暗号解除装置２から出力された圧縮データに対して第１の暗号鍵を使用して暗号化を行い、第１暗号データＡ１を出力する第１暗号化装置である。符号４は、第１の暗号鍵を生成して第１の暗号化装置３に提供し、また、認証鍵を使用して第１の暗号鍵を暗号化し、その認証鍵に基づいた相互認証の完了を条件として該暗号化された第１の暗号鍵を出力する認証装置である。この認証装置４は、無効な認証鍵の情報が記載された無効化鍵リストＤ１を有し、この無効化鍵リストＤ１の中に相互認証に使用する認証鍵の情報が含まれる場合には当該認証を不可とする。符号５は、放送信号に含まれる無効化対象の認証鍵の情報を放送受信装置１から受け取ると、その情報に基づいて認証装置４の無効化鍵リストＤ１を更新する無効鍵更新装置である。

【００３１】符号６は、メモリおよびＣＰＵ（中央処理装置）等により構成され、プログラムをメモリにロードして実行することによりその機能を実現する処理装置である。この処理装置６は、第１暗号解除部１１と画像音声伸張部１２と認証部１３と認証鍵更新部１４のそれぞれの機能を実現するためのプログラムを実行する。

【００３２】第１暗号解除部１１は、第１暗号データＡ１を受け取り、当該暗号化に使用された第１の暗号鍵を使用してその暗号を解除する。画像音声伸張部１２は、第１暗号解除部１１によって暗号が解除された圧縮データを受け取り、このデータに対して伸張処理を行う。この伸張処理によって圧縮データは再生可能な画像データ及び音声データとなる。画像音声伸張部１２は、伸張された画像データ及び音声データの再生処理も行うことが可能である。

【００３３】認証部１３は、認証装置４との間でデータＡ２を送受して相互認証を行い、この認証完了により認証装置４から第１暗号解除部１１で使用する第１の暗号鍵を取得する。この認証部１３は、認証装置４との間の相互認証に使用する認証鍵を有している。認証鍵更新部１４は、放送信号に含まれる更新用認証鍵を放送受信装置１から受け取ると、認証部１３の認証鍵を更新する。また、認証鍵更新部１４は、放送信号に含まれる更新用プログラムを放送受信装置１から受け取ると、第１暗号解除部１１と画像音声伸張部１２と認証部１３と自部１４のそれぞれの処理プログラム（第１の暗号解除処理プログラム、画像音声伸張処理プログラム、認証処理プログラム、認証鍵更新処理プログラム）を更新する。

【００３４】符号７は、放送暗号解除装置２から出力された圧縮データに対して第２の暗号鍵を使用して暗号化を行い、第２暗号データＢ１を出力する第２暗号化装置である。この第２暗号化装置７は、暗号化に使用した第２の暗号鍵を自装置内に保持する。符号８は、第２暗号化装置７から暗号化に使用された第２の暗号鍵を受け取り、その暗号を解除する第２暗号解除装置である。

【００３５】符号９は、第２暗号化装置７から第２暗号データＢ１を受け取ると、記録媒体に記録する記録装置である。この記録装置９としては、ハードディスク装置や光磁気ディスク装置、あるいはＤＶＤ（Digital Versatile Disc）等の記録媒体の読み書き装置などが利用可能である。

【００３６】なお、上記処理装置６には、周辺機器として入力装置、表示装置、スピーカ等（いずれも図示せず）が接続されるものとする。ここで、入力装置とはキーボード、マウス等の入力デバイスのことをいう。表示装置とはＣＲＴ（Cathode RayTube）や液晶表示装置等のことをいう。このような処理装置６としては、パーソナルコンピュータや携帯情報端末などの情報処理装置が利用可能である。

【００３７】また、上記図１に示す装置の内、装置１～５、７及び８を一つの装置として構成するようにしてもよい。例えば、装置１～５、７及び８のそれぞれの機能を実現する電子回路を一つの基板上に実装し、これを処理装置６及び記録装置９と接続するようにする。このようにすれば、その基板をパーソナルコンピュータ等の情報処理装置に実装して図１の著作権保護システムを実現することが可能となる。

【００３８】なお、上記図１に示す装置３～５、７及び８は専用のハードウェアにより実現されるものであってもよい。また、それら装置３～５、７及び８はメモリおよびＣＰＵ（中央処理装置）により構成され、装置３～５、７及び８の各々の機能を実現するためのプログラムをメモリにロードして実行することによりその機能を実現させるものであってもよい。このようにＣＰＵ等からなるコンピュータを利用して実現する場合には、読出し専用のメモリ（ＲＯＭ）にプログラムを格納するようにすれば、プログラムの改竄を防止することが可能であ

る。あるいは、ＣＰＵやメモリ等を内臓したＬＳＩ（システムＬＳＩ）により、それら装置３～５、７及び８を実現するようにしてもよい。

【００３９】次に、図１に示す著作権保護システムの動作を説明する。初めに、放送信号を受信してその放送内容を再生する動作について説明する。先ず、放送受信装置１は放送信号を受信すると、圧縮暗号化データを出力し、放送暗号解除装置２がその暗号を解除して圧縮データを出力する。

【００４０】次いで、第１暗号化装置３は、放送暗号解除装置２から圧縮データを受け取ると、認証装置４から提供された第１の暗号鍵を使用して暗号化を行い、第１暗号データＡ１を出力する。ここで使用される第１の暗号鍵は、処理装置６との間で共有される鍵である。なお、この第１の暗号鍵を共有する動作については後述する。

【００４１】次いで、処理装置６の第１暗号解除部１１は、第１暗号化装置３から第１暗号データＡ１を受け取ると、第１暗号化装置３との間で共有された第１の暗号鍵を使用してその暗号を解除する。画像音声伸張部１２は、第１暗号解除部１１により暗号が解除された圧縮データを受け取ると、伸張処理を行い、画像または音声を再生する。

【００４２】上述したように本実施形態においては、第１暗号化装置３から処理装置６へ出力されるデータ（第１暗号データＡ１）は暗号化されたものなので、第１暗号化装置３と処理装置６の間を接続する伝送媒体（データ伝送可能なバス等）からデータを取得しても、そのデータから再生可能な著作物のデータを取得することは困難である。

【００４３】次に、図２を参照して、上記第１の暗号鍵を共有する動作について説明する。この第１の暗号鍵の共有処理は認証装置４と認証部１３の間で行われるが、その際、認証装置４と認証部１３は認証鍵に基づいた相互認証を行う。図２は、第１の暗号鍵の共有処理の流れを示すフローチャートであって、公開鍵暗号方式による相互認証により第１の暗号鍵の共有する場合の例を示す。図２に示すように、認証装置４は、公開鍵ｐ１、公開鍵証明書ｃ１、秘密鍵ｓ１、無効化鍵リストＤ１、及び公開鍵ｐｃを有している。また、認証部１３は、公開鍵ｐ２、公開鍵証明書ｃ２、秘密鍵ｓ２、及び公開鍵ｐｃを有している。

【００４４】上記公開鍵証明書ｃ１は、第三者機関（認証局）により、この第三者機関（認証局）が有する秘密鍵ｓｃで予め公開鍵ｐ１に署名が付加され発行されたものであり、この署名を公開鍵ｐｃで検証する。同様に第三者機関により、公開鍵証明書ｃ２は、秘密鍵ｓｃで予め公開鍵ｐ２に署名が付加され発行されたものであり、この署名を公開鍵ｐｃで検証する。これら署名により、公開鍵証明書ｃ１、ｃ２の偽造が防止される。

【００４５】公開鍵ｐ１と秘密鍵ｓ１は対を成す認証鍵である。同様に、公開鍵ｐ２と秘密鍵ｓ２も対を成す認証鍵となっている。なお、上記公開鍵ｐ２と秘密鍵ｓ２は、認証装置４と認証部１３の間の相互認証に用いられる認証鍵の一つであり、認証装置４が行う第１の暗号鍵の暗号化に係る鍵となるものである。また、無効化鍵リストＤ１には、無効な公開鍵証明書ｃ２を示す情報が記載されている。この無効化鍵リストＤ１についても、偽造を防ぐために、第三者機関が有する秘密鍵ｓｃで署名が付加され発行される。

【００４６】先ず、認証装置４は乱数Ｒ１を生成して認証部１３へ送信する（図２のステップＳＰ１、ＳＰ２）。次いで、認証部１３は、受け取った乱数Ｒ１に対して秘密鍵ｓ２で署名Ｓｉｇ（ｓ２，Ｒ１‖ＩＤ２）を作成する。この署名Ｓｉｇ（ｓ２，Ｒ１‖ＩＤ２）を作成する際には、番号ＩＤ２として公開鍵証明書ｃ２のシリアル番号を用いるようにしてもよい。また、認証部１３は乱数Ｒ２を生成する。次いで、認証部１３は、作成した署名Ｓｉｇ（ｓ２，Ｒ１‖ＩＤ２）と公開鍵証明書ｃ２と乱数Ｒ２を認証装置４へ送信する（図２のステップＳＰ３～ＳＰ５）。

【００４７】なお、上記記号「‖」はビットの連結を示す。例えば、「Ｒ１‖ＩＤ２」は乱数Ｒ１と番号ＩＤ２がビット連結されたビット列を示し、署名Ｓｉｇ（ｓ２，Ｒ１‖ＩＤ２）はそのビット列「Ｒ１‖ＩＤ２」に対して秘密鍵ｓ２で署名が付加されたものである。また、上記乱数Ｒ１、Ｒ２としては、熱雑音を使用してもよく、あるいは擬似乱数を使用してもよい。ただし、擬似乱数を使用する場合には、認証装置４と認証部１３にそれぞれ擬似乱数生成器を備えるようにするが、それら擬似乱数生成器が不一致のものとなるようにする。

【００４８】次いで、認証装置４は、受け取った公開鍵証明書ｃ２が無効化鍵リストＤ１に未記載であることを確認する。ここで、受け取った公開鍵証明書ｃ２が無効化鍵リストＤ１に記載されていた場合には、認証装置４は、当該公開鍵ｐ２が無効なものであると判断し、認証部１３との認証を不可とし、認証未完了のままその処理を終了する。一方、受け取った公開鍵証明書ｃ２が無効化鍵リストＤ１に未記載であった場合には、認証装置４は相互認証を継続し、以下の処理を行う（図２のステップＳＰ６）。

【００４９】次いで、認証装置４は、公開鍵証明書ｃ２を公開鍵ｐｃで検証する。また、公開鍵ｐ２と乱数Ｒ１により署名Ｓｉｇ（ｓ２，Ｒ１‖ＩＤ２）を検証する。ここで認証装置４は、これら検証の結果がいずれか一つでも異常であった場合には、認証部１３との認証を不可とし、認証未完了のままその処理を終了する（図２のステップＳＰ７、ＳＰ８）。

【００５０】一方、認証装置４は、それら検証の結果が全て正常であった場合には、乱数Ｒ２に対して秘密鍵ｓ

１で署名Ｓｉｇ（ｓ１，Ｒ２‖ＩＤ１）を作成する。この署名Ｓｉｇ（ｓ１，Ｒ２‖ＩＤ１）を作成する際には、番号ＩＤ１として公開鍵証明書ｃ１のシリアル番号を用いるようにしてもよい（図２のステップＳＰ９）。

【００５１】次いで、認証装置４は、第１の暗号鍵Ｋ１を生成し、この第１の暗号鍵Ｋ１を公開鍵ｐ２で暗号化して暗号Ｅｎｃ（ｐ２，Ｋ１）を生成する。また、認証装置４は、その生成した第１の暗号鍵Ｋ１を第１暗号化装置３へ提供する。次いで、認証装置４は、署名Ｓｉｇ（ｓ１，Ｒ２‖ＩＤ１）と公開鍵証明書ｃ１と暗号Ｅｎｃ（ｐ２，Ｋ１）を認証部１３へ送信する（図２のステップＳＰ１０～ＳＰ１２）。

【００５２】次いで、認証部１３は、受け取った公開鍵証明書ｃ１を公開鍵ｐｃで検証する。また、公開鍵ｐ１と乱数Ｒ２により署名Ｓｉｇ（ｓ１，Ｒ２‖ＩＤ１）を検証する。ここで認証部１３は、これら検証の結果がいずれか一つでも異常であった場合には、認証装置４との認証を不可とし、認証未完了のままその処理を終了する（図２のステップＳＰ１３、ＳＰ１４）。

【００５３】一方、認証部１３は、それら検証の結果が全て正常であった場合には、暗号Ｅｎｃ（ｐ２，Ｋ１）を秘密鍵ｓ２で復号して第１の暗号鍵Ｋ１を取得し、この第１の暗号鍵Ｋ１を第１暗号解除部１１へ提供する（図２のステップＳＰ１５）。これにより、認証装置４によって生成された第１の暗号鍵Ｋ１が、第１暗号化装置３と第１暗号解除部１１の間で共有されたことになる。

【００５４】なお、上述した実施形態においては、第１の暗号鍵の共有処理における認証を公開鍵暗号方式による相互認証により行うようにしたが、その認証方法は公開鍵暗号方式に限定されるものではない。

【００５５】次に、認証部１３が有している認証鍵を無効化する動作を説明する。この無効化対象の認証鍵とは、認証装置４と認証部１３の間の相互認証に用いられる認証鍵の一つであって、認証装置４が行う第１の暗号鍵の暗号化に係る鍵となるものである。上記図２に示す公開鍵暗号方式による相互認証の例においては、公開鍵ｐ２と秘密鍵ｓ２のことを指す。

【００５６】悪意を持った第三者が、図１の著作権保護システムの認証部１３の認証鍵を不正に取得し、この認証鍵を用いて認証装置４と第１の暗号鍵を共有して第１暗号データＡ１の暗号を解除し、放送番組の画像や音声などの著作物を不正に使用する場合がある。このような場合には、放送事業者は、これ以上の著作物不正使用を防止するために無効化対象の認証鍵の情報と更新用認証鍵を放送信号に含めて放送する。以下、図１の著作権保護システムの動作を説明する。

【００５７】放送受信装置１は、受信した放送信号に無効化対象の認証鍵の情報が含まれている場合には、その情報を無効鍵更新装置５へ出力する。無効鍵更新装置５

は、放送受信装置１から無効化対象の認証鍵の情報を受け取ると、この情報に基づいて認証装置４の無効化鍵リストＤ１を更新する。これにより、認証部１３が有する認証鍵は無効化されたことになる。

【００５８】また、放送受信装置１は、受信した放送信号に更新用認証鍵が含まれている場合には、その更新用認証鍵を処理装置６の認証鍵更新部１４へ出力する。認証鍵更新部１４は、放送受信装置１から更新用認証鍵を受け取ると、認証部１３の認証鍵を更新する。これにより、認証部１３が有する認証鍵は有効な認証鍵となる。

【００５９】したがって、悪意を持った第三者が不正に取得した認証鍵により著作物を使用する場合には、認証装置４と認証部１３の間で第１の暗号鍵を共有する際に無効化された認証鍵が使用されることになるので、認証装置４は、上記図２のステップＳＰ６において認証部１３との間の相互認証を不可とし、第１の暗号鍵を認証部１３へ提供しない。この結果、第１暗号解除部１１は、第１暗号化装置３により暗号化に使用された第１の暗号鍵を取得することができず、第１暗号データＡ１の暗号を解除することができなくなる。これにより、たとえ悪意を持った第三者により、認証方式や暗号化方式が解読されて著作物が不正に使用されたとしても、認証鍵（暗号に係る鍵）を無効化して、これ以上のさらなる著作物の不正使用を防止することができるという効果が得られる。

【００６０】また、上述したように本実施形態による著作権保護システムによれば、放送信号に含めて提供される無効化対象の認証鍵の情報と更新用認証鍵により、認証鍵の無効化とその変更を行う。したがって、放送事業者は、著作物の不正使用を防止するために無効化対象の認証鍵の情報と更新用認証鍵を放送信号に含めて放送するだけで、認証鍵の無効化とその変更を簡易に実施することができる。

【００６１】このように、放送される画像データや音声データなどの著作物に係る入力データに付随して提供される無効化対象の認証鍵の情報や更新用認証鍵により、暗号に係る鍵（認証鍵）の無効化とその変更を行うようにすれば、当該著作物に係る入力データを使用する複数の著作権保護システムに対して、暗号に係る鍵の無効化とその変更を一斉に行うことが可能となる。この結果、当該著作物の不正使用に対する対処を能率よく実施することができるという効果が得られる。

【００６２】また、放送事業者は、処理装置６の第１暗号解除部１１と画像音声伸張部１２と認証部１３と認証鍵更新部１４のそれぞれの処理プログラム（第１の暗号解除処理プログラム、画像音声伸張処理プログラム、認証処理プログラム、認証鍵更新処理プログラム）を更新可能な更新用プログラムを放送信号に含めて放送するようにしてもよい。この場合には、放送受信装置１は受信した更新用プログラムを認証鍵更新部１４へ出力し、認

証鍵更新部１４がその更新用プログラムによりぞれぞれの処理プログラムを更新する。このように処理装置６の処理プログラムを更新するようにすれば、当該処理プログラムが不正に改竄されて使用された場合においても、改竄された処理プログラムのさらなる不正使用を防止することが可能となる。

【００６３】次に、図１に示す著作権保護システムが放送信号を受信してその放送内容を記録し、また記録された放送内容を再生する動作について説明する。先ず、放送受信装置１は放送信号を受信すると、圧縮暗号化データを出力し、放送暗号解除装置２がその暗号を解除して圧縮データを出力する。

【００６４】次いで、第２暗号化装置７は、放送暗号解除装置２から圧縮データを受け取ると、第２の暗号鍵を使用して暗号化を行い、第２暗号データＢ１を出力する。第２暗号化装置７は、暗号化の契機がある度に乱数等を利用して第２の暗号鍵を生成し、自装置７内に保持する。記録装置９は、第２暗号化装置７から第２暗号データＢ１を受け取ると、記録媒体へ記録する。

【００６５】この記録されたデータを再生する場合には、先ず、記録装置９が記録媒体から第２暗号データＢ２を読み出して出力する。第２暗号解除装置８は、この第２暗号データＢ２を受け取ると、その暗号化に使用された第２の暗号鍵を第２暗号化装置７から取得し、第２暗号データＢ２の暗号を解除して第１暗号化装置３へ出力する。次いで、上述した第１の暗号鍵による暗号化に係る過程を経た後、画像音声伸張部１２によって、記録装置９により記録された放送内容が再生されることになる。

【００６６】なお、上述した実施形態においては、第２暗号解除装置８への第２の暗号鍵の提供方法として、第２暗号化装置７が暗号化の契機がある度に乱数等を利用して第２の暗号鍵を生成し、この第２の暗号鍵を自装置７内に保持するようにしたが、第２の暗号鍵を記録装置９により記録するようにしてもよい。ただし、この場合には、自システムにおいてのみその記録した第２の暗号鍵を使用可能となるようにする。例えば、第２暗号化装置７毎に異なる固有のＩＤ（識別番号）と、第２の暗号鍵との所定演算の結果を第２暗号データＢ１に付加して記録する。この場合には、第２暗号解除装置８は、第２暗号化装置７からそのＩＤを取得し、第２暗号データＢ１に付加された演算結果と取得したＩＤにより、第２の暗号鍵を復元して取得する。

【００６７】上記いずれかの第２の暗号鍵の提供方法により第２の暗号鍵を第２暗号解除装置８に提供するようにしておけば、たとえ図１に示す著作権保護システムから記録装置９を取り外して同様の構成を備えた他の著作権保護システムに取り付けたとしても、正しい第２の暗号鍵を得ることは困難であり、記録した著作権保護システム以外のシステムでは再生不可とすることができるようになる。この結果、著作物そのものが不正に複製されることを抑止するという効果が得られる。

【００６８】なお、上記いずれかの第２の暗号鍵の提供方法により、記録した著作権保護システム以外のシステムでは再生不可とするようにしておいてもよいし、あるいは他の方法を用いてもよい。例えば、記録媒体からの読出し自体にシステム固有の認証を必要とするようにしてもよい。

【００６９】また、上述した実施形態によれば、記録に係る装置７～９と再生に係る装置３～６とを独立に備えるようにしたので、記録処理と再生処理を同時におこなうタイムシフトと呼ばれる処理も行うことができる。

【００７０】上述したように本実施形態によれば、記録時の暗号化方式（第２の暗号鍵による方式）と再生時の暗号化方式（第１の暗号鍵による方式）にそれぞれ異なる方式を用いるのようにしたので、たとえ再生時の第１の暗号が解読され、著作物の記録または再生が不正に行われたとしても、記録時の第２の暗号が直接解読されることを防止することは可能である。したがって、再生時の第１の暗号に係る鍵（認証鍵）を変更することによって、これ以上は不正に著作物が記録または再生されることを防止することができる。また、第２の暗号で記録されたデータについては、以前と同様に再生が可能である。この結果、利用者の利便性を損なうことなく、記録再生に係る著作権保護を実施することができるという効果が得られる。

【００７１】なお、上述した実施形態においては、著作権保護対象の著作物を画像または音声とし、暗号化対象の著作物に係る入力データとして画像データまたは音声データを例にして説明したが、他の著作物に対しても同様に適用可能である。例えば、小説等の文章を著作権保護対象の著作物とする場合には、著作物に係る入力データをテキストデータとして適用すればよい。

【００７２】また、上述した実施形態においては、著作物に係る入力データを放送信号に含めて配信する場合について説明したが、著作物に係る入力データの取得方法は、放送形式で配信される場合に限定されるものではない。例えば、著作権保護システムの利用者がインターネット等の通信ネットワークを介して著作物に係る入力データを自ら取得するようにしてもよい。この場合には、図１の装置１、２の代わりに、通信ネットワーク接続装置（モデムやダイヤルアップルータ等）とその通信データに係る暗号解除装置を備えるようにする。

【００７３】あるいは、著作物に係る入力データを記録媒体を介して取得するようにしてもよい。例えば、ＤＶＤに記録された著作物のデータを著作物に係る入力データとしてもよい。この場合には、図１の装置１、２の代わりに、ＤＶＤの読出し装置とその読出しデータに係る暗号解除装置を備えるようにする。

【００７４】なお、上述した実施形態においては、図１

の第１暗号化装置３が第１の暗号化手段に対応し、第１暗号解除部１１が第１の暗号解除手段に対応する。また、認証装置４が認証手段に対応し、認証装置４の無効化鍵リストＤ１の記載内容が暗号に係る鍵の無効情報に対応する。また、無効鍵更新装置５が無効情報更新手段に対応する。

【００７５】また、処理装置６の認証鍵更新部１４が認証鍵更新手段に対応する。また、処理装置６が暗号化の解除に係る機能を実現するための処理プログラムを実行する処理装置に対応する。また、第１暗号解除部１１と画像音声伸張部１２と認証部１３と認証鍵更新部１４のそれぞれの処理プログラム（第１の暗号解除処理プログラム、画像音声伸張処理プログラム、認証処理プログラム、認証鍵更新処理プログラム）が暗号化の解除に係る機能を実現するための処理プログラムに対応する。

【００７６】また、第２暗号化装置７が第２の暗号化手段に対応し、第２暗号解除装置８が第２の暗号解除手段に対応する。

【００７７】また、図１に示す装置３～８が行う各処理を実現するためのプログラムをコンピュータ読み取り可能な記録媒体に記録して、この記録媒体に記録されたプログラムをコンピュータシステムに読み込ませ、実行することにより著作権保護処理を行ってもよい。なお、ここでいう「コンピュータシステム」とは、ＯＳや周辺機器等のハードウェアを含むものであってもよい。また、「コンピュータシステム」は、WWWシステムを利用している場合であれば、ホームページ提供環境（あるいは表示環境）も含むものとする。また、「コンピュータ読み取り可能な記録媒体」とは、フレキシブルディスク、光磁気ディスク、ＲＯＭ、ＣＤ－ＲＯＭ、メモリカード等の可搬媒体、コンピュータシステムに内蔵されるハードディスク等の記憶装置のことをいう。

【００７８】さらに「コンピュータ読み取り可能な記録媒体」とは、インターネット等のネットワークや電話回線等の通信回線を介してプログラムが送信された場合のサーバやクライアントとなるコンピュータシステム内部の揮発性メモリ（ＲＡＭ）のように、一定時間プログラムを保持しているものも含むものとする。また、上記プログラムは、このプログラムを記憶装置等に格納したコンピュータシステムから、伝送媒体を介して、あるいは、伝送媒体中の伝送波により他のコンピュータシステムに伝送されてもよい。ここで、プログラムを伝送する「伝送媒体」は、インターネット等のネットワーク（通信網）や電話回線等の通信回線（通信線）のように情報を伝送する機能を有する媒体のことをいう。また、上記プログラムは、前述した機能の一部を実現するためのものであっても良い。さらに、前述した機能をコンピュータシステムにすでに記録されているプログラムとの組み合わせで実現できるもの、いわゆる差分ファイル（差分プログラム）であっても良い。

【００７９】以上、本発明の実施形態を図面を参照して詳述してきたが、具体的な構成はこの実施形態に限られるものではなく、本発明の要旨を逸脱しない範囲の設計変更等も含まれる。

【００８０】

【発明の効果】以上説明したように、本発明によれば、暗号に係る鍵の無効情報を有し、第１の暗号化手段と第１の暗号解除手段の間で暗号化に係る第１の暗号鍵を共有する際の認証に使用する認証鍵の情報が無効情報の中に含まれる場合に、当該認証を不可とする。また、著作物に係る入力データに付随して提供される無効化対象の鍵の情報を受け取ると、無効情報の内容を更新する。これにより、自システム内の暗号に係る鍵を無効化することが可能となる。さらに、著作物に係る入力データを使用する複数の著作権保護システムに対して、暗号に係る鍵の無効化を一斉に行うことが可能となる。この結果、著作物の不正使用に対する対処を能率よく実施することができるという効果も得られる。

【００８１】さらに、著作物に係る入力データに付随して提供される更新用認証鍵により、認証鍵を更新するようにすれば、複数の著作権保護システムにおいてそれらの暗号に係る鍵（認証鍵）を簡易に変更することができる。

【００８２】また、著作物に係る入力データに付随して提供される更新用プログラムを受け取り、この更新用プログラムにより、暗号化の解除に係る機能を実現するための処理プログラムを更新するようにすれば、複数の著作権保護システムにおいてそれらの暗号に係るプログラムを簡易に変更することができる。

【００８３】また、第２の暗号鍵を使用して著作物に係る入力データを暗号化し、該第２の暗号データを記録媒体に記録するようにすれば、記録時の暗号化方式（第２の暗号鍵による方式）と再生時の暗号化方式（第１の暗号鍵による方式）にそれぞれ異なる方式を用いることが可能となり、たとえ再生時の第１の暗号が解読され、著作物の記録または再生が不正に行われたとしても、記録時の第２の暗号が直接解読されることを防止することは可能である。したがって、再生時の第１の暗号に係る鍵（認証鍵）を変更することによって、これ以上は不正に著作物が記録または再生されることを防止することができる。また、第２の暗号で記録されたデータについては、以前と同様に再生が可能である。この結果、利用者の利便性を損なうことなく、記録再生に係る著作権保護を実施することができるという効果が得られる。

【００８４】さらに、第２の暗号鍵を自システム内に保持し、第２の暗号データの暗号を自システム内に保持された第２の暗号鍵により解除するようにすれば、著作物を記録した著作権保護システム以外のシステムではその記録データを再生不可とすることができるようになる。この結果、著作物そのものが不正に複製されることを抑

止するという効果が得られる。

【図面の簡単な説明】

【図１】　本発明の一実施形態による著作権保護システムの構成を示すブロック図である。

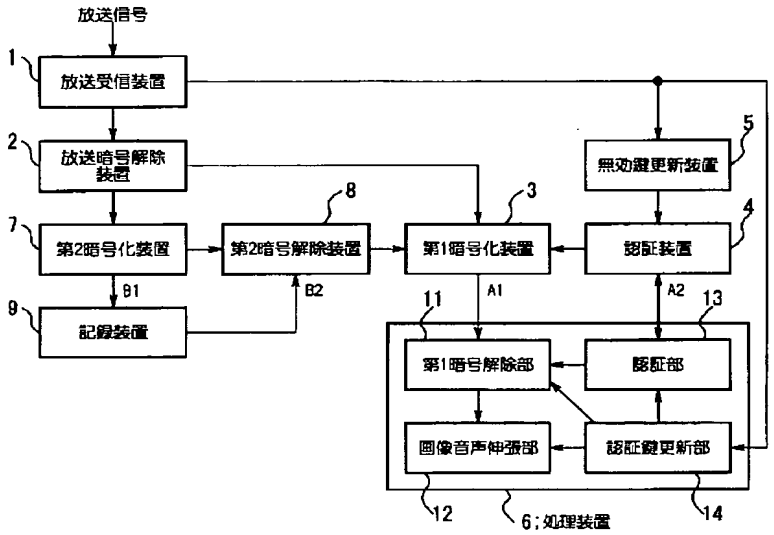
【図２】　図１に示す著作権保護システムが行う第１の暗号鍵の共有処理の流れを示すフローチャートである。

【図３】　従来の著作権保護システムの構成例を示すブロック図である。

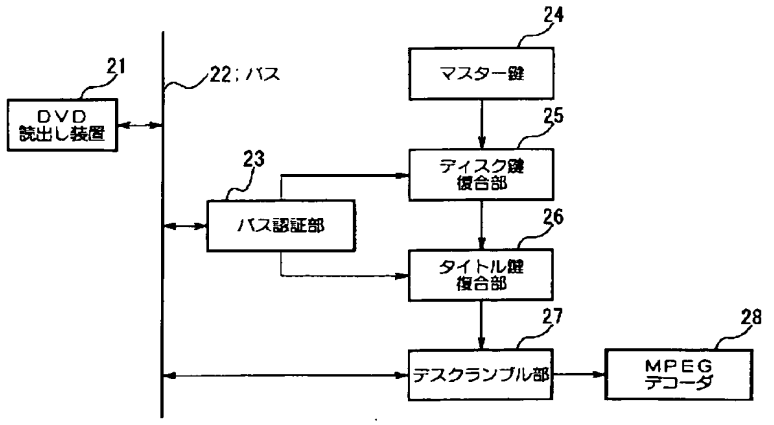
【符号の説明】

１　放送受信装置
２　放送暗号解除装置
３　第１暗号化装置
４　認証装置
５　無効鍵更新装置
６　処理装置
７　第２暗号化装置
８　第２暗号解除装置
９　記録装置
１１　第１暗号解除部
１２　画像音声伸張部
１３　認証部
１４　認証鍵更新部
Ｄ１　無効化鍵リスト

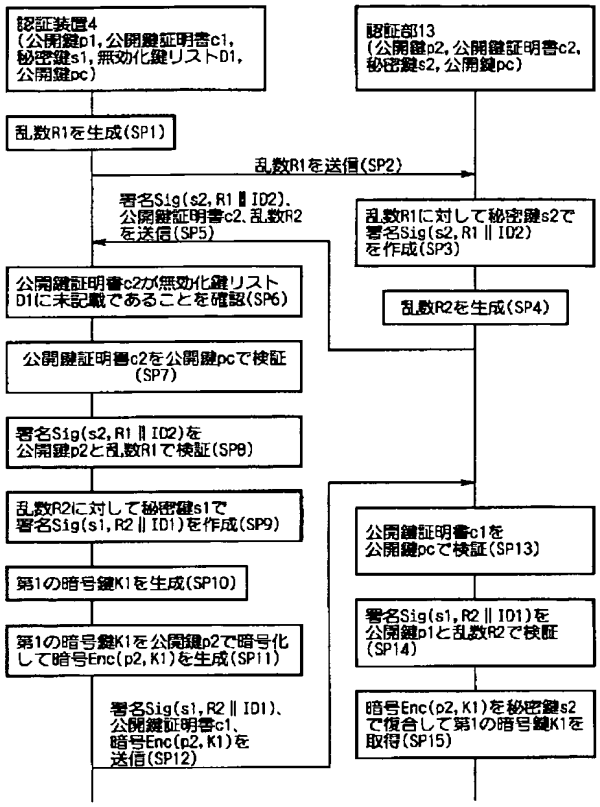
【図１】



【図３】



【図２】



フロントページの続き

(72)発明者　峯松　一彦
東京都港区芝五丁目７番１号　日本電気株式会社内

(72)発明者　尾花　賢
東京都港区芝五丁目７番１号　日本電気株式会社内

Ｆターム(参考)　5B017 AA07 BA07 CA15
5J104 AA01 AA07 AA16 AA41 BA03
EA01 EA04 KA04 NA02 PA05